10/519698
DT01 Rec'd PCT/PTO 27 DEC 2004

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application.

Claim 1 (currently amended): A cryptographic method ~~that can be used in~~ for a transaction ~~for which~~ whereby a first entity ~~(A)~~ generates, by means of an RSA private key ~~(d)~~, a proof verifiable by a second entity ~~(B)~~ by means of an RSA public key associated with said private key, said public key comprising a first exponent ~~(e)~~ and a modulus ~~(n)~~, the method comprising the steps of ~~characterized in that~~:

- generating a first element of proof at the first entity, whereby ~~(A) generates a first element of proof (x), a first~~ calculation of said first element of proof is executable ~~which, consuming considerable resources, can be executed~~ independently of the transaction;
- generating, at the first entity, ~~(A) generates~~ a second element of proof ~~(y)~~ related to the first element of proof ~~(x)~~ and dependent on a common number ~~(e)~~ shared by the first and second entities specifically for the transaction, ~~a second~~ whereby calculation of ~~which~~ said first element of proof consumes ~~few~~ substantially less resources than the calculation of said first element of proof; and
- verifying, at the second entity ~~(B) verifies~~ that the first element of proof ~~(x)~~ is related through a relationship with a first power modulo the modulus ~~(n)~~ of a generic number ~~(g)~~ having a second exponent equal to a linear combination of ~~all or~~ at least part of the common number ~~(e)~~ and of the first exponent ~~(e)~~ of the public key multiplied by the second element of proof ~~(y)~~.

Claim 2 (currently amended): The cryptographic method as claimed in claim 1, ~~characterized in that, to allow~~ wherein for identifying the first entity, ~~(A) to be identified:~~

- the first element of proof ~~(x)~~ is generated by the first entity ~~(A)~~ by raising the generic number ~~(g)~~ to a second power modulo the modulus ~~(n)~~ having a third exponent equal to the first exponent ~~(e)~~ of the public key multiplied by a random integer ~~(r)~~ kept secret by the first entity, wherein ~~(A);~~

- the common number ~~(e)~~ is chosen randomly from within a security interval [0,t 1] and then sent by the second entity ~~(B)~~ after having received the first element of proof, ~~(x);~~ and wherein
- the relationship verified by the second entity ~~(B)~~ is an equality relationship between a power of the first element of proof ~~(x)~~ and the first power of the generic number ~~(g)~~.

Claim 3 (currently amended): The cryptographic method as claimed in claim 1, ~~characterized in that, in order to allow~~ wherein for signing a message, ~~(M) to be signed:~~

- the first element of proof ~~(x)~~ is generated by the first entity ~~(A)~~ by applying a ~~standard~~ hash function to the message ~~(M)~~ and to the generic number ~~(g)~~ raised to a second power modulo the modulus ~~(n)~~ having a third exponent equal to the first exponent ~~(e)~~ of the public key multiplied by a random integer ~~(r)~~ kept secret by the first entity, wherein ~~(A);~~
- the common number ~~(e)~~ is equal to the first element of proof, ~~(x);~~ and wherein
- the relationship verified by the second entity ~~(B)~~ is an equality relationship between the first element of proof ~~(x)~~ and a result of ~~the standard~~ said hash function applied to the message ~~(M)~~ and to the first power of the generic number ~~(g)~~.

Claim 4 (currently amended): The cryptographic method as claimed in claim 1, ~~characterized in that, in order to allow~~ wherein for authenticating that a message ~~(M)~~ received by the second entity ~~(B)~~ comes from the first entity, ~~(A):~~

- the first element of proof ~~(x)~~ is generated by the first entity ~~(A)~~ by applying a ~~standard~~ hash function to the message ~~(M)~~ and to the generic number ~~(g)~~ raised to a second power modulo the modulus ~~(n)~~ having a third exponent equal to the first exponent ~~(e)~~ of the public key multiplied by a random integer ~~(r)~~ kept secret by the first entity, wherein ~~(A);~~
- the common number ~~(e)~~ is chosen at random from within a security interval [0,t 1] and then sent by the second entity ~~(B)~~ after having received the first element of proof, ~~(x);~~ and wherein

- the relationship verified by the second entity ~~(B)~~ is an equality relationship between the first element of proof ~~(x)~~ and a result of ~~the standard~~ said hash function applied to the message ~~(M)~~ and to the first power of the generic number ~~(g)~~.

Claim 5 (currently amended): The cryptographic method as claimed in ~~one of claims 2 to~~ claim 4, wherein ~~characterized in that:~~

- the second element of proof ~~(y)~~ is generated by the first entity ~~(A)~~ by subtracting, from the random integer ~~(r)~~, the private key ~~(d)~~ multiplied by the common number, wherein ~~(e);~~
- the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number ~~(e)~~ and a positive unitary coefficient for the first exponent ~~(e)~~ of the public key multiplied by the second element of proof, ~~(y);~~ and wherein,
- in the verified relationship, the first element of proof is considered with a unitary exponent power.

Claim 6 (currently amended): The cryptographic method as claimed in ~~either of claims 2 and~~ claim 4, ~~characterized in that:~~

- ~~since~~ wherein the common number ~~(e) is split into a~~ comprises first ~~elementary common number (a)~~ and ~~a~~ second elementary common ~~number (b)~~ numbers, wherein the second element of proof ~~(y)~~ is generated by the first entity ~~(A)~~ by subtracting, from the random integer ~~(r)~~ multiplied by the first elementary common number ~~(a)~~, the private key ~~(d)~~ multiplied by the second elementary common number, ~~(b);~~
- wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number ~~(a)~~, a positive unitary coefficient for the second elementary common number ~~(b)~~ and a positive unitary coefficient for the first exponent ~~(e)~~ of the public key multiplied by the second element of proof, ~~(y); and~~
- and wherein, in the verified relationship, the first element of proof is considered with an exponent power equal to the first elementary common number ~~(a)~~.

Claim 7 (currently amended): The cryptographic method as claimed in ~~either of claims 5 and~~ claim 6, ~~characterized in that~~ wherein the second element of proof ~~(y)~~ is calculated modulo an image of the modulus ~~(n)~~ via a Carmichael function ~~(λ)~~ or modulo a multiple of the order of the generic number ~~(g)~~ modulo the modulus ~~(n)~~.

Claim 8 (currently amended): The cryptographic method as claimed in ~~either of claims 5 and~~ claim 6, ~~characterized in that~~ wherein the random number ~~(r)~~ is ~~very much~~ substantially greater than the value of the private key ~~(d)~~.

Claim 9 (currently amended): The cryptographic method as claimed in claim 7, ~~characterized in that~~ wherein the random integer ~~(r)~~ is less than an image of the modulus ~~(n)~~ via a Carmichael function ~~(λ)~~ or less than a multiple of the order of the generic number ~~(g)~~ modulo the modulus ~~(n)~~.

Claim 10 (currently amended): The cryptographic method as claimed in ~~one of claims 5 to 9, characterized in that~~ claim 9, wherein the third exponent is calculated modulo an image of the modulus ~~(n)~~ via a Carmichael function ~~(λ)~~ or modulo a multiple of the order of the generic number ~~(g)~~ modulo the modulus ~~(n)~~.

Claim 11 (currently amended): The cryptographic method as claimed in ~~one of the preceding claims, characterized in that~~ claim 1, wherein the generic number ~~(g)~~ is transmitted with the public key, the generic number ~~(g)~~ being equal to a simple number ~~(G)~~ raised to a power modulo the modulus ~~(n)~~ with the private key ~~(d)~~ as exponent.

Claim 12 (currently amended): The cryptographic method as claimed in ~~one of the preceding claims, characterized in that~~ claim 1, further comprising the steps of:

- receiving the second element of proof at a third entity; ~~(C) receives the second element of proof (y), generates~~
- generating a third element of proof ~~(Y)~~ at the third entity by raising the generic number ~~(g)~~ to a power modulo the modulus ~~(n)~~ with the second element of proof ~~(y)~~ as exponent; ~~and sends~~

- sending the third element of proof ~~(Y)~~ to the second entity ~~(B)~~; and
- at ~~the~~ second entity, raising ~~(B), modulo the modulus (n), raises~~ the third element of proof ~~(Y)~~ to a power of first exponent, modulo the modulus, ~~(e)~~ and ~~multiplies~~ multiplying the result thereof by the generic number ~~(g)~~ raised to a power whose exponent is the common number ~~(e)~~ in order to verify the relationship relating the first element of proof to the second element of proof.

Claim 13 (currently amended): A prover device ~~(30) provided with~~ having an RSA private key ~~(d)~~ kept secret and protected against intrusions, for generating, during a transaction with a verifier device, a proof whose verification by means of a public key associated with said private key ~~makes it possible to guarantee~~ ensures that ~~the~~ said prover device ~~(30)~~ has originated said proof, said RSA public key comprising a first exponent ~~(e)~~ and a modulus ~~(n),~~ ~~characterized in that it comprises~~, the prover device comprising:

- calculation means ~~(37) designed to generate~~ for generating a first element of proof ~~(x)~~ completely or partly independently of the transaction and to generate a second element of proof ~~(y)~~ related to the first element of proof and dependent on a common number ~~(e)~~ specific to the transaction; and
- communication means ~~(34) designed to transmit~~ for transmitting at least the first and second elements of proof and ~~designed to transmit~~ for transmitting said common number ~~(e)~~ to the verifier device or ~~to receive~~ receiving said common number ~~therefrom~~ from the verifier device.

Claim 14 (currently amended): The prover device ~~(30)~~ as claimed in claim 13, ~~characterized in that:~~

- wherein the calculation means ~~(37)~~ are, on the one hand, designed to generate a first random number ~~(r)~~ and to raise a generic number ~~(g)~~ to a second power modulo the modulus ~~(n)~~ having a third exponent equal to the first exponent ~~(e)~~ of the public key multiplied by the random integer ~~(r)~~; and
- wherein the calculation means ~~(37)~~ are, on the other hand designed to generate the second element of proof ~~(y)~~ by taking the difference between the random integer ~~(r)~~ and the private key ~~(d)~~ multiplied by the common number ~~(e)~~ or, where the common

number ~~(c) being~~ is split into two elementary common numbers ~~(a, b)~~, by subtracting from the random integer ~~(r)~~ multiplied by the first elementary common number ~~(a)~~, the private key ~~(d)~~ multiplied by the second elementary common number ~~(b)~~.

Claim 15 (currently amended): The prover device ~~(30)~~ as claimed in claim 14, ~~characterized in that~~ wherein the calculation means ~~(37)~~ are designed to carry out operations modulo an image of the modulus ~~(n)~~ via a Carmichael function ~~(λ)~~ or modulo a multiple of the order of the generic number ~~(g)~~ modulo the modulus ~~(n)~~.

Claim 16 (currently amended): A verifier device ~~(31)~~ for verifying that a proof originates from a prover device provided with an RSA private key ~~(d)~~ kept secret by the prover device, by means of a public key associated with said private key, said RSA public key comprising an exponent ~~(e)~~ and a modulus ~~(n), characterized in that it comprises~~, the verifier device comprising:

- communication means ~~(35) designed to receive~~ for receiving a first element of proof ~~(x)~~ and a second element of proof ~~(y)~~ or a third element of proof ~~(Y)~~, and ~~to receive or transmit~~ for receiving or transmitting a common number ~~(e)~~ specific to a transaction within which the first and the second or the third element of proof are received; and
- calculation means ~~(38) designed to verify~~ for verifying that the first element of proof ~~(x)~~ is related through a relationship, modulo the modulus ~~(n)~~, with a first power of a generic number ~~(g)~~ having a second exponent equal to a linear combination of ~~all or~~ at least part of the common number ~~(e)~~ and of the first exponent ~~(e)~~ of the public key multiplied by the second element of proof ~~(y)~~.

Claim 17 (currently amended): The verifier device ~~(31)~~ as claimed in claim 16, ~~characterized in that~~ wherein the communication means are designed to receive the second element of proof ~~(y)~~ and ~~in that~~ wherein the calculation means ~~(38)~~ are designed to calculate the second exponent and said first power of the generic number ~~(g)~~.

Claim 18 (currently amended): The verifier device ~~(31)~~ as claimed in claim 16, ~~characterized in that~~ wherein the communication means are designed to receive the third element of proof

~~(Y)~~ and ~~in that~~ wherein the calculation means ~~(38)~~ are designed to raise the third element of proof ~~(Y)~~ to a power of the first exponent ~~(e)~~ of the public key in order to multiply the result thereof by the generic number ~~(g)~~ raised to a second power having the common number ~~(e)~~ as exponent.

Claim 19 (new): The cryptographic method as claimed in claim 2, wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number, wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the first exponent of the public key multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power.

Claim 20 (new): The cryptographic method as claimed in claim 19, wherein the second element of proof is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 21 (new): The cryptographic method as claimed in claim 20, wherein the random integer is less than an image of the modulus via a Carmichael function or less than a multiple of the order of the generic number modulo the modulus.

Claim 22 (new): The cryptographic method as claimed in claim 19, wherein the third exponent is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 23 (new): The cryptographic method as claimed in claim 3, wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number, wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the first exponent of the public key multiplied by the second

element of proof, and wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power.

Claim 24 (new): The cryptographic method as claimed in claim 23, wherein the second element of proof is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 25 (new): The cryptographic method as claimed in claim 24, wherein the random integer is less than an image of the modulus via a Carmichael function or less than a multiple of the order of the generic number modulo the modulus.

Claim 26 (new): The cryptographic method as claimed in claim 23, wherein the third exponent is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 27 (new): The cryptographic method as claimed in claim 2, wherein the common number comprises first and second elementary common numbers, wherein the second element of proof is generated by the first entity by subtracting, from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number, wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number, a positive unitary coefficient for the second elementary common number and a positive unitary coefficient for the first exponent of the public key multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with an exponent power equal to the first elementary common number.

Claim 28 (new): The cryptographic method as claimed in claim 27, wherein the second element of proof is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 29 (new): The cryptographic method as claimed in claim 28, wherein the random integer is less than an image of the modulus via a Carmichael function or less than a multiple of the order of the generic number modulo the modulus.

Claim 30 (new): The cryptographic method as claimed in claim 27, wherein the third exponent is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.